

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306301

(43)Date of publication of application : 05.11.1999

(51)Int.Cl. G06K 17/00
G06K 19/07
G06K 19/073

(21)Application number : 10-110924 (71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 21.04.1998 (72)Inventor : YANO YOSHIHIRO
HANDA FUKIO
HAYASHI MASAHIRO
MAKINO HIROSHI

(54) IC CARD HAVING SECURITY STATUS WITH TIME LIMIT

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an IC card from being illegally used after expiration by a person other than the genuine owner.

SOLUTION: With respect to an IC card having a timer function a security status indicating an authentication valid state is kept only for a prescribed time after expiration of the authentication of a card owner and the term of validity of the card owner authentication is set to a master key file IEF00 and application key files IEF01IEF02 and IEF03.

CLAIMS

[Claim(s)]

[Claim 1]An IC card wherein security status which shows a card holder's attestation effective state after the end of attestation maintains only predetermined time in an IC card which has an arithmetic unit main memory read-only memory nonvolatile memory and a timer function.

[Claim 2]An IC card characterized by returning security status or making it blockade an applicable application file after the above-mentioned predetermined time passed.

[Claim 3]An IC card setting the term of validity of card holder attestation as a key file

in the IC card according to claim 1 or 2.

[Claim 4]An IC card setting up the term of validity of card holder attestation for every application file in the IC card according to claim 1 or 2 at a key file.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the IC card which prevented the continuous illegal use of the IC card by persons other than a true card holder.

[0002]

[Description of the Prior Art]As shown in drawing 4the reader/writer 1 transmits a command (command) to IC card 2and the IC card which received this interprets a commandand performs processing of writing/read-outand it returns it to the reader/writer 1 by making a processing result into a response.

[0003]As shown in drawing 5IC card 2 has CPU2aRAM2bROM2cand EEPROM2d.

If the command which reads into CPU2a the program memorized by ROM2cand is transmitted from the reader/writer 1 is received through an I/O PortThe data transmitted with the command is readrequired processing is performeda result is written in the predetermined file area of EEPROM2dand a response is outputted through an I/O Port.

the time check which will apply to which and notify interruption to CPU2a if 2e is a timer moduleand operates independently of operation of CPU2a and the set-up time passes --- it is a device.

[0004]Drawing 6 is what showed EEPROM3 which consists of a field for application programsand a field for operating system (OS)When assigning the file of the application ABand C in this order from the start address of an application areaA directoryB directoryand C directory are simultaneously formed toward a head in order of assignment of file area from the last of an application area. A directory is the control information on a fileand as shown in drawing 7it consists of file ID for identifying a filethe start address a file is remembered to beare capacityattribution information (information on the right to access (key) of read/write)and a check code.

[0005]In drawing 6in the field for OS which followed the field of application. The data which OS of the pointer in which the address of the last of the assigned file area is shown from the start address shown in the directory and area capacitythe pointer in which the directory of the accumulated last is shownetc. uses is set. The field between the pointer P and P' is a memory area which can further be assigned.

[0006]As shown in drawing 8the command from reader/writer The classification (CLA) of a commandThe data length Lc and a data division (file IDarea capacityattribution information) are added to a command (INS)the parameter P1and P2and assignment of

a file is performed by a creation file operation.

[0007]

[Problem(s) to be Solved by the Invention]The key (PIN:Personal Identification Number) which the card holder inputted from the terminal in the conventional IC card is compared with the key stored in the IC card. Since security status was updated when in agreement, access to a file was possible for after it on the level with which it is satisfied of security attributes until the IC card was deactivated (state where the card was extracted from the contact).

[0008]In drawing 9, key file IEF00 directly under a master file Express a card holder key and AP1, AP2 and AP3 show the application program file in dedicated file DF. IEF01, IEF02 and IEF03 are key files in which key PIN1 for accessing each application program. PIN2 and PIN3 are stored respectively.

[0009]If PIN which the card holder's attestation (global security status) was performed at the time of the PIN input to the key directly under MF and was inputted is in agreement with the key of IEF00, unless the global status shown in drawing 10 is updated from 0 to 1 and a card holder's performs authentication is clearly carried out by the IC card utilizing system side (contact side) after it. Or unless it is deactivated by the IC card side, the first global security status is held.

[0010]When the power for accessing each dedicated file is lodged, for example, it accesses application AP1 in this state. It compares with PIN1 of key file IEF01 and if this agrees, it will become accessible to AP1. At this time, the security status of drawing 10 is updated from 0 to 1. Security status is the authority that the application file concerned can be accessed and does not reach to other applications.

[0011]Thus, since the first global security status will be held once performs authentication is successful. Even if it exchanges a challenge/response (procedure which passes a random number mutually by the contact and the IC card side and checks whether a partner is genuine), the performs authentication of the bona fides of a card. There was no means to detect even if the person who is operating it toward a contact has changed from the just card holder to another inaccurate operator who attested at the time of the original PIN input.

[0012]Thus, as a situation which changes the person who is operating it toward a contact to an unjust person from a genuine card holder. The situation forgotten to telephone inserting the IC card of SIM (Subscriber Identification Module) in a failure to extract and portable telephone of the IC card in a POS register terminal is assumed.

[0013]It is for this invention solving an aforementioned problem and aims at preventing the continuous illegal use of the IC card by persons other than a true card holder.

[0014]

[Means for Solving the Problem]In an IC card which has an arithmetic unit, main memory, read-only memory, nonvolatile memory and a timer function, this invention maintained only time predetermined in security status which shows a card holder's

attestation effective state after the end of attestation. After this invention passed the above-mentioned predetermined time it returns security status or it was made to blockade an applicable application file. This invention set the term of validity of card holder attestation as a key file. This invention set the term of validity of card holder attestation to every application file as a key file.

[0015]

[Embodiment of the Invention] Hereafter an embodiment of the invention is described. The IC card of this invention is the same as that of the thing of composition of having been shown in drawing 5 and has a timer function. It is a mechanism in which CPU2a is told about this timer function having measured lapsed time using the clock supplied from the outside and the time of the specified term of validity having passed and it does not matter even if it realizes by dedicated hardware and the interval timer by software realizes.

[0016] This invention provides the term of validity in security status (attestation effective state) When the effective state of the security status after the card holder attestation by a card holder's PIN input continues only fixed time and security status returns before card holder attestation after fixed time lapse it keeps the continuous use after it from being possible. Although setting out of the term of validity is set up to global security status and all the security status of each application in the example explained below Setting out of the term of validity is not limited to this and receives the security status of global security status or each application for example Or it may be made to perform setting up to the security status of important specific application etc. suitably.

[0017] it is shown in drawing 1 -- as -- key file IEF00 directly under MF key file IEF01 under each application file IEF02 and IEF03 -- the record of the term of validity is attached to respectively. When it may be set up from the beginning or necessity arises after that it may be made to set up this term of validity. For example if key file IEF00 directly under MF is specified with an authentication command After memorizing the present global security status after comparing the value of the key in inputted PIN and a file if in agreement global security status is updated and a timer function is made to start. The term of validity directed to a timer function is called for by four operations such as the sum of the term of validity (it is the term of validity of the whole card and sets up beforehand for example) of IEF00 and the term of validity recorded on IEF01 or a difference when using application AP1. When using application AP2 it asks by four operations recorded on each of IEF00 and IEF02 such as the sum of the term of validity or a difference. The term of validity of IEF00 also does a certain operation and it may be made to ask for it. Thus the term of validity of card holder attestation can be set as variable for every application. Of course each term of validity may be set up by a method like other throats.

[0018] Drawing 2 is a figure showing the example of a card holder attestation process flow and the arrow with which the arrow which goes to right-hand side from left-hand

side goes to left-hand side from the command from the terminal side to an IC card and right-hand side shows the response sent to the terminal side from an IC card. In [in A1 a card holder chooses application and] A2 The SELECT file command (file selection command) which chooses AP1 is sent to an IC card and in the case of normal termination a status word (9000) is returned as a response from the IC card side in A3. Next in [in V1 a card holder inputs PIN into a terminal and] V2 An authentication command (PIN which parameter = IEF00 IEF01 and a data division = card holder inputted) is sent and in V3 by the IC card side collation of PIN and a timer set are performed and if it is normal termination a status word (9000) will be returned as a response. In this state the right to access of AP1 is acquired and mutual command/response are performed by the protocol peculiar to application after P1. In Pn if the security status term of validity passes in the meantime in order not to fill security status the status word 6982 will be returned and it will return to a card holder attestation front. And in order to carry out continuous use further the process of above V1 and V2 must be performed.

[0019] Drawing 3 is a figure showing the example of authentication command processing and shows the process flow in the case of acquiring the right to access of AP1. If IEF00 and IEF01 are specified with an authentication command and access to AP1 is tried. If IEF00 is searched first and IEF00 is found the present security status will be memorized in a memory and the data division (value of PIN which the card holder inputted) of a command and the record value of IEF00 will be compared (Step S1 - S4). If collation is in agreement IEF01 will be searched next and if IEF01 is found the term of validity T of security status will be computed (Steps S5-S8). Subsequently a timer function is called and argument T is set as a timer (setting out of the term of validity). Subsequently a response is edited (Step S10) and the response of normal termination is returned (Step S11). In this way since the term of validity is set up if this term expires it must stop having to fill security status and in the case of continuous use authenticating processing must be performed again. In Step S5 when collation of IEF00 goes wrong it flies to Step S10 the contents of a response are edited and an error is returned.

[0020]

[Effect of the Invention] As mentioned above according to this invention even when it crosses to the hand of a user with an inaccurate terminal unit which inserted the IC card after the PIN input attestation by a genuine IC card holder continuous use of the IC card by an illegal use person can be prevented. In the system which must attest a card holder strictly especially by the system using an IC card for example an electronic cash system Since the IC card itself returns security status to the state before the collation attestation by a card holder's PIN periodically by using the IC card of this invention Even if it crosses to an illegal use person's hand it becomes impossible to satisfy the security attributes of an important cash information file and a continuous

illegal use can be prevented.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a figure explaining the file structure of this invention.

[Drawing 2] It is a figure showing the example of a card holder attestation process flow.

[Drawing 3] It is a figure showing the example of authentication command processing.

[Drawing 4] It is a figure explaining communication of reader/writer and an IC card.

[Drawing 5] It is a figure explaining the composition of an IC card.

[Drawing 6] It is a figure explaining the composition of EEPROM.

[Drawing 7] It is a figure explaining the composition of a directory.

[Drawing 8] It is a figure explaining the composition of a command.

[Drawing 9] It is a figure showing a file structure.

[Drawing 10] It is a figure explaining security status.

[Description of Notations]

1 [-- Timer.] -- Reader/writer 2 -- An IC card 2 a--CPU 2 a--RAM 2 b -- ROM 2 d--EEPROM 2 e
